INFORMATION AND CONTROL 33, 56–71 (1977)

Semiregular Convolutional Codes: Definition, Structure, and Examples

PHILIPPE DELSARTE AND PHILIPPE PIRET

MBLE Research Laboratory, Brussels, Belgium

In this paper, the set of sequences of q-ary n-tuples is endowed with the structure of a module over an appropriate algebra. Then, semiregular convolutional codes are introduced as submodules; such codes indeed have the property that they admit a semiregular automorphism group. The structure and properties of the codes are investigated in detail. In particular, some canonical generators are exhibited that can be used to construct a minimal encoder. Finally, several examples are given which show that there actually exist good semiregular convolutional codes.

1. INTRODUCTION

In coding theory, a great amount of research has been devoted to the study of some classes of *block codes* having a rich algebraic structure. For example, the usual *cyclic codes*, which are defined by the property of admitting a cyclic regular automorphism group, have the well-known structure of *ideals* in an appropriate *group algebra*. More generally, let G be any group of order r, and C any linear block code of length $n = rm$ over a finite field F, with the properties that G acts on the n coordinate positions of C as a *semiregular permutation group* (cf. Wielandt, 1964) and leaves C invariant. Then the code C may be viewed as a *submodule* of the *free module* $(FG)^m$, that is the direct product of m copies of the group algebra FG. We especially refer to MacWilliams (1967) for the regular case, i.e., $m = 1$, where the codes simply are ideals of FG. Let us also mention two special families, which both are natural generalizations of cyclic codes and have been studied in the literature: *Abelian codes*, defined from an Abelian group G and $m = 1$ (cf., for instance, MacWilliams, 1970), and *quasicyclic codes*, corresponding to a cyclic group G and any $m \geqslant 1$ (cf. Chen, Peterson, and Weldon, 1969).

For *convolutional codes*, the situation is rather different. Since the fundamental paper by Forney (1970), the general structure of codes of this type is well understood. But, so far, most known constructions are mainly of an

algorithmic nature. And, even if these methods are efficient, the resulting codes do not have some specific algebraic structure, comparable to the ones mentioned above for block codes. Recently, however, there has been a first attempt to fill this gap; and a concept of *cyclic convolutional codes* has been introduced by Piret (1976). The present work is concerned with a generalization of this notion; the definition of semiregularity is extended to the case of convolutional codes.

Roughly, the idea is the following. Let $B = FG$ be the group algebra of the group G over the field aphabet F, and let $B(D)$ denote the vector space of all sequences with coefficients in B. Next, for any fixed automorphism of G, we define a multiplication on $B(D)$ that gives it the structure of a *linear associative algebra.* Then, given an integer $m \geqslant 1$, a convolutional code of block length $n = rm$ over F is called *semiregular* whenever it is a *submodule* of the *free module* $(B(D))^m$. The main emphasis in this paper is put on questions of structure, but without omission of the "practical aspects": under some weak assumptions, the analysis of a semiregular convolutional code produces certain *canonical generators* from which a minimal encoder can be built up (cf. Forney, 1970). On the other hand, several examples are given at the end of the paper. They show that there do exist some very good codes with the required properties. Moreover, it turns out that the investigation of a class of codes with given "small parameters" is relatively easy, and the computation of their *free distance* is not too difficult.

As indicated in this introduction, the general context of our study is the theory of modules and group algebras. For this matter, the reader is referred to Curtis and Reiner (1962).

2. Convolutional Codes and Modules

Given a set A, let $A(D)$ denote the set of *sequences* in an indeterminate D, with coefficients in A, that is,

$$A(D) = \left\{ a(D) = \sum_{i=\sigma}^{\infty} a_i D^i;\ a_i \in A,\ \sigma \in \mathbb{Z} \right\}. \tag{1}$$

In particular, let F be a field. Then $F(D)$ itself forms a field, for the usual operations, namely the quotient field of the ring of formal power series in D.

For an integer $n \geqslant 1$, the set $(F(D))^n = F^n(D)$ of all n-tuples over $F(D)$ has the structure of an n-dimensional vector space. When F is the finite field $GF(q)$, for some prime power q, any k-dimensional subspace of $F^n(D)$ over $F(D)$ will be called a *q-ary (n, k) convolutional code*, provided it is generated

by a set of sequences with finitely many nonzero terms. This definition is essentially "equivalent" to the classical notion, for which we refer to Forney (1970).

Before introducing the concepts of regularity for convolutional codes, we need some notations from the theory of group algebras. Let G be a finite group whose order r is a divisor of the *block length* n, and let $m = n/r$. Then we can write the n-tuples $\mathbf{g}$ over F as follows:

$$\mathbf{g} = (g^1(x), g^2(x), \ldots, g^m(x))_{\forall x \in G}, \tag{2}$$

for some fixed numbering of the elements x of G, where g^s denotes any mapping from G to F. It will be convenient to represent such a mapping $a: G \to F$ by the formal sum

$$a = \sum_{x \in G} xa(x), \qquad a(x) \in F. \tag{3}$$

The set B of all expressions (3) has the obvious structure of a vector space over F, isomorphic to F^r. Moreover, defining a multiplication $(a, b) \mapsto ab$ on B by the rule

$$(ab)(x) = \sum_{y \in G} a(y)\, b(y^{-1}x), \tag{4}$$

we make B an associative algebra, called the *group algebra* of G over F. Notice that, if G is a cyclic group ($\simeq \mathbb{Z}_r$), then B can be interpreted as the algebra $F[z]/(z^r - 1)$ of polynomials in z reduced modulo $z^r - 1$.

With these notations, a convolutional code of block length $n = rm$ may be viewed as a set of m-tuples whose components are sequences over B. Indeed, let B^m denote the Cartesian product of m copies of B. Then a convolutional code appears to be an $F(D)$-subspace of $(B(D))^m = B^m(D)$, where $B(D)$ and $B^m(D)$ are defined as in (1). More precisely, according to (2) and (3), we identify an element $\mathbf{g}(D) = \sum \mathbf{g}_i D^i$ of $B^m(D)$ with the following n-tuple in $F^n(D)$:

$$\mathbf{g}(D) = \left(\sum_i g_i^1(x)\, D^i, \ldots, \sum_i g_i^m(x)\, D^i \right)_{\forall x \in G}, \tag{5}$$

for $\mathbf{g}_i = (g_i^1, \ldots, g_i^m) \in B^m$ and $g_i^s = \sum x\, g_i^s(x) \in B$.

So far, we did not use the group structure of G. We shall now do so. Let $\pi: x \mapsto x^\pi$ be a permutation on G. We use the same notation for the extension of π to the group algebra B, that is,

$$a \mapsto a^\pi = \sum_{x \in G} x^\pi a(x), \qquad \text{for} \quad a \in B. \tag{6}$$

Let now $(\beta(j); j \in \mathbb{Z})$ be a fixed collection of permutations $\beta(j)$ on G, with $1^{\beta(j)} = 1$. To this we associate a binary operation $\circ$ on $B(D)$ by defining

$$a(D) \circ b(D) = \sum_{i,j} (a_i^{\beta(j)} b_j)\, D^{i+j}, \tag{7}$$

for all $a(D)$, $b(D) \in B(D)$, the products $a_i^{\beta(j)} b_j$ being performed in B (cf. (4) and (6)). Note that (7) reduces to the usual multiplication in the field $F(D)$ as well as in the group algebra B, viewed as subsets of $B(D)$. Let us now define the action of $B(D)$ on $B^m(D)$ by pointwise left multiplication:

$$a(D) \circ \mathbf{g}(D) = (a(D) \circ g^1(D), \ldots, a(D) \circ g^m(D)), \tag{8}$$

for all $a(D)$ in $B(D)$ and $\mathbf{g}(D) = (g^1(D), \ldots, g^m(D))$ in $B^m(D)$.

Roughly, we are interested in any convolutional code $M \subset B^m(D)$ that is invariant under multiplication by $B(D)$, in the sense of (8). However, not all choices of the $\beta(j)$ are suitable for our purpose; we want the multiplication (7) to be *associative*. In this case, $B(D)$ has the structure of a *linear F-algebra*. Hence $B^m(D)$ becomes a left $B(D)$-module, of which M appears as a *submodule*.

THEOREM 2.1. *The system $(B(D), +, \circ)$ is a linear algebra over the field F if and only if $\beta(i) = \alpha^i$ holds, for all $i \in \mathbb{Z}$, where α is some fixed automorphism of G.*

Proof. Assume $\circ$ is associative. Then, given any elements x and y in G and any integer i, we may write

$$D^{-i} \circ (xy) \circ D^i = (D^{-i} \circ x \circ D^i) \circ (D^{-i} \circ y \circ D^i). \tag{9}$$

Now (7) yields $D^{-i} \circ z \circ D^i = z^{\beta(i)}$, for all $z \in G$. Applying this identity to both members of (9) we obtain $(xy)^{\beta(i)} = x^{\beta(i)} y^{\beta(i)}$, which means that $\beta(i)$ is an automorphism of G. Next, we use

$$D^{-i-j} \circ x \circ D^{i+j} = D^{-j} \circ (D^{-i} \circ x \circ D^i) \circ D^j. \tag{10}$$

Application of $D^{-i} \circ z \circ D^i = z^{\beta(i)}$ to (10) yields $\beta(i+j) = \beta(i)\,\beta(j)$, for all $i, j \in \mathbb{Z}$. The solutions to these equations clearly have the form $\beta(i) = \alpha^i$ for an arbitrary α in $\mathrm{Aut}(G)$. The rest of the proof is by straightforward verification and will not be given. ∎

DEFINITION 2.2. Let $\beta(i) = \alpha^i$ with $\alpha \in \mathrm{Aut}(G)$. A convolutional code $M \subset B^m(D)$ will be said to be *semiregular*, of type (G, α, m), if $B(D) \circ M$ equals M, i.e., if $a(D) \circ \mathbf{g}(D)$ belongs to M for all $\mathbf{g}(D)$ in M and all $a(D)$ in $B(D)$.

From now on we shall always take $\beta(i) = \alpha^i$, for some $\alpha \in \mathrm{Aut}(G)$, so that $B(D)$ actually is an F-algebra (cf. Theorem 2.1). We point out that $B(D)$ is generally not an $F(D)$-algebra. However, the $B(D)$-submodules of $B^m(D)$ clearly are vector spaces over the field $F(D)$. In particular, semiregular convolutional codes exactly are those submodules of $B^m(D)$ having finite generators.

We now make a simple remark. Let G' be a subgroup of G such that $(G')^\alpha = G'$ holds. Then a semiregular code of type (G, α, m) may also be viewed as being of type (G', α', m'), where α' is the restriction of α to G' and m' equals $m[G : G']$. A detailed verification of this correspondence is left to the reader. Notice also that a code of type $(\{1\}, 1, n)$ is any convolutional code of block length n.

Our terminology in Definition 2.2 is motivated by the following observation. A convolutional code M is semiregular, for a given G, if and only if M is invariant under the action of G as a *semiregular permutation group* on the coordinate positions. In the present context, this means that, for any sequence $\mathbf{g}(D) \in M$, its images

$$x \circ \mathbf{g}(D) = \sum_i (x^{\beta(i)}\mathbf{g}_i)\, D^i$$

also belong to M, for all elements x of G. In the case $m = 1$, the codes M of our definition should be called *regular*. They are the left *ideals* of $B(D)$. In particular, regular codes with a cyclic group $G \cong \mathbb{Z}_n$ are *cyclic convolutional codes* in the sense of Piret (1976). For an arbitrary m and for $G \cong \mathbb{Z}_r$, a semiregular code could be called *quasicyclic*, in analogy to the usual terminology for block codes. Thus our concepts of regular and semiregular convolutional codes are rather natural extensions of the corresponding notions in the theory of block codes. The only intriguing point perhaps is the presence of the automorphisms $\beta(i) = \alpha^i$ in the definition. We point out that, for given G and m, the most interesting codes often correspond to a choice of $\alpha \neq 1$.

We shall now give a result allowing simplification of an exhaustive search for all inequivalent algebras defined on $B(D)$. Let $\circ$ and $*$ be the product operators (7) associated to $\beta(i) = \alpha^i$ and to $\beta(i) = \gamma^i$, respectively, where α and γ are given automorphisms of G. The algebras $(B(D), +, \circ)$ and $(B(D), +, *)$ are called *isomorphic* if there exists a permutation π on G satisfying

$$(a(D) * b(D))^\pi = (a(D))^\pi \circ (b(D))^\pi, \tag{11}$$

for all $a(D), b(D) \in B(D)$, where the π-image of any $c(D)$ in $B(D)$ is defined

to be $(c(D))^{\pi} = \sum c_i^{\pi} D^i$. In this situation, the semiregular convolutional codes of type (G, γ, m) are essentially the same as those of type (G, α, m).

THEOREM 2.3. *If α and γ are conjugate in* Aut(G), *then the corresponding algebras* $(B(D), +, \circ)$ *and* $(B(D), +, *)$ *are isomorphic.*

Proof. Let $\gamma = \pi\alpha\pi^{-1}$, with $\pi \in \mathrm{Aut}(G)$. Then the theorem follows from definitions (7) and (11), by straightforward verification. ∎

Let us finally examine the question of duality for semiregular convolutional codes. Given any two vectors $\mathbf{g}, \mathbf{h} \in F^n = B^m$, written as in (2), their *inner product* in F is given by

$$(\mathbf{g}, \mathbf{h}) = \sum_{x \in G} \sum_{s=1}^{m} g^s(x)\, h^s(x). \tag{12}$$

The inner product $B^m(D) \times B^m(D) \to F(D)$ is constructed from (12) by natural extension. Thus, for all $\mathbf{g}(D)$, $\mathbf{h}(D)$ in $B^m(D)$, we have

$$(\mathbf{g}(D), \mathbf{h}(D)) = \sum_{i,j} (\mathbf{g}_i\,, \mathbf{h}_j)\, D^{i+j}. \tag{13}$$

The *dual* $M^{\perp}$ of any (n, k) convolutional code M is its orthogonal complement, i.e., the set of sequences $\mathbf{h}(D) \in B^m(D)$ such that $(\mathbf{g}(D), \mathbf{h}(D)) = 0$ holds for all $\mathbf{g}(D)$ in M. Clearly, $M^{\perp}$ is an $(n, n - k)$ convolutional code.

THEOREM 2.4. *Let M be a semiregular code of type (G, α, m). Then its dual $M^{\perp}$ is a semiregular code of type (G, α^{-1}, m).*

Proof. Denote by $\circ$ and $*$ the product operators (7) associated to $\beta(i) = \alpha^i$ and to $\beta(i) = \alpha^{-i}$, respectively. From the property $(x\mathbf{g}, \mathbf{h}) = (\mathbf{g}, x^{-1}\mathbf{h})$ of the inner product (12) it follows that the condition $(z \circ \mathbf{g}(D), \mathbf{h}(D)) = 0$ for all $z \in G$ is equivalent to $(\mathbf{g}(D), y * \mathbf{h}(D)) = 0$ for all $y \in G$ (cf. (7) and (13)). This implies the assertion. ∎

3. STRUCTURE OF SEMIREGULAR CONVOLUTIONAL CODES

Our main objective in this section is to find certain canonical generators for semiregular convolutional codes. We recall that these codes are any $B(D)$-submodules of $B^m(D)$ generated by sequences with finitely many nonzero terms. Let

$$\mathbf{g}(D) = \sum_{i=\sigma}^{\sigma+\nu-1} \mathbf{g}_i D^i, \qquad \text{with} \quad \sigma \in \mathbb{Z},\ \nu \in \mathbb{N} \cup \{\infty\},\quad \mathbf{g}_i \in B^m,$$

be a sequence of $B^m(D)$. (When $\nu = 0$ this means $\mathbf{g}(D) = \mathbf{0}$.) For the above writing, σ will be called the *index* and ν the *length* of $\mathbf{g}(D)$. The m-tuples $\mathbf{g}_i$ are the *words* of $\mathbf{g}(D)$ and $\mathbf{g}_\sigma$ is the *initial word.* We shall now introduce a concept that plays a crucial role in our study.

DEFINITION 3.1. A nonzero sequence $\mathbf{h}(D)$ of index 0 is said to be *normal* if it satisfies the following condition:

$$(a\mathbf{h}_0 = \mathbf{0}) \Rightarrow (a \circ \mathbf{h}(D) = \mathbf{0}), \qquad \text{all } a \in B.$$

Our first result is a general expression for normal sequences, showing how they are characterized by their initial word. Thereafter, we shall exhibit two useful properties of the $B(D)$-modules generated by normal sequences.

THEOREM 3.2. *A sequence* $\mathbf{h}(D)$, *with given initial word* $\mathbf{h}_0 = \mathbf{h} \neq \mathbf{0}$, *is normal if and only if there exist B-endomorphisms* A_i *of* B^m *satisfying*

$$\mathbf{h}(D) = \sum_{i=0}^{\infty} (\mathbf{h}A_i)^{\beta(i)} D^i. \tag{14}$$

Proof. Define $J = \sum (h^s B)$ to be the right ideal of B generated by the components $h^s \in B$ of the word $\mathbf{h} = (h^1, \ldots, h^m)$. Let a be any element of B satisfying $a\mathbf{h} = \mathbf{0}$, i.e., $a \in l(J) =$ left annihilator of J. Applying (7) we obtain

$$a \circ \mathbf{h}(D) = \sum_{i=1}^{\infty} (a\mathbf{f}_i)^{\beta(i)} D^i, \qquad \text{with} \quad \mathbf{f}_i = \mathbf{h}_i^{\beta(-i)}.$$

Assume $\mathbf{h}(D)$ is normal. Writing $\mathbf{f}_i = (f_i^1, \ldots, f_i^m)$, we must have $af_i^s = 0$ for every i, s and every $a \in l(J)$. In other words, the f_i^s belong to the right annihilator $r(l(J))$ of $l(J)$, which is nothing but J itself (cf. Curtis and Reiner, 1962, p. 402). Thus we may write

$$f_i^s = \sum_{t=1}^{m} h^t a_{i,t}^s, \qquad \text{for some} \quad a_{i,t}^s \in B.$$

In matrix form this becomes $\mathbf{f}_i = \mathbf{h}A_i$, with $A_i \in \mathrm{End}_B(B^m)$. Hence the direct part of the theorem is proved. Conversely, it is quite obvious that any sequence (14) is normal. ∎

LEMMA 3.3. *The* $B(D)$*-module* $B(D) \circ \mathbf{h}(D)$ *generated by a normal sequence* $\mathbf{h}(D)$ *is irreducible if and only if* $B\mathbf{h}_0$ *is an irreducible B-module.*

Proof. Assume $B\mathbf{h}_0$ is irreducible. Let $a(D) \in B(D)$ be such that $a_0\mathbf{h}_0 \neq \mathbf{0}$ holds, together with $a_i = 0$ for all $i < 0$. If we are able to exhibit an element $b(D)$ of $B(D)$ satisfying

$$b(D) \circ a(D) \circ \mathbf{h}(D) = \mathbf{h}(D), \tag{15}$$

then we certainly may assert that $B(D) \circ \mathbf{h}(D)$ is irreducible. It turns out that condition (15), together with $b_i = 0$ for $i < 0$, is equivalent to the following triangular system:

$$b_i a_0 \mathbf{h}_0 = \begin{cases} \mathbf{h}_0, & i = 0, \\ \left(-\sum_{j=1}^{i} b_{i-j}^{g(j)} a_j\right) \mathbf{h}_0, & i \geqslant 1. \end{cases}$$

This result, which is a generalization of the long division in $F(D)$, is easily obtained by the use of Theorem 3.2 (or simply Definition 3.1). Now, if we assume $B\mathbf{h}_0$ is irreducible, then it is clear that the above system admits a solution for the b_i. Hence the "if proposition" is proved. The converse result is rather obvious and its proof will be omitted. ▮

LEMMA 3.4. *Let $\mathbf{h}_1(D),\ldots, \mathbf{h}_t(D)$ be normal sequences having the property that the sum of the B-modules $B\mathbf{h}_s$ generated by their initial words $\mathbf{h}_s\,(= \mathbf{h}_{s,0})$ is a direct sum. Then the sum of the $B(D)$-modules $B(D) \circ \mathbf{h}_s(D)$ also is direct.*

Proof. We have to show that, if $\sum a_s(D) \circ \mathbf{h}_s(D) = \mathbf{0}$ holds for some $a_1(D),\ldots, a_t(D)$ in $B(D)$, then each term $a_s(D) \circ \mathbf{h}_s(D)$ must be zero. Without loss of generality, we may assume $a_{s,i} = 0$ when $i < 0$. Then it can be readily verified, by use of Theorem 3.2 or Definition 3.1, that $\sum a_s(D) \circ \mathbf{h}_s(D) = \mathbf{0}$ is equivalent to

$$\sum_{s=1}^{t} a_{s,i}\mathbf{h}_s = \mathbf{0}, \qquad \text{all} \quad i \geqslant 0.$$

By assumption, this implies $a_{s,i}\mathbf{h}_s = \mathbf{0}$ (for every s), and, consequently, $a_s(D) \circ \mathbf{h}_s(D) = \mathbf{0}$. Hence the lemma is proved. ▮

Before giving the main theorems, we need a preliminary result concerning the presence of normal sequences in semiregular codes. This requires a few more definitions and notations. As usual, a module is said to be *completely reducible* if every submodule is a direct summand. The *socle* of the B-module B^m, hereafter denoted by $S(B^m)$, is the unique maximal completely reducible

submodule of B^m. Thus $S(B^m)$ coincides with B^m if and only if B is semi-simple, i.e., if and only if $|G|$ and $|F|$ are relatively prime. Incidentally, we point out that the same condition is a criterion for complete reducibility of the $B(D)$-module $B^m(D)$.

DEFINITION 3.5. A nonzero semiregular convolutional code $M \subset B^m(D)$ will be said to be *locally reducible* if the words of all its sequences belong to the socle $S(B^m)$. Equivalently, M is locally reducible when its words form a completely reducible B-module.

Let M be a semiregular convolutional code, $M \neq (\mathbf{0})$. For any non-negative integer ν, we define M_ν to be the B-module formed by the sequences of index 0 and length ν in M. We shall denote by P_ν the *projection* of M_ν in B^m, i.e., the set of initial words of the sequences belonging to M_ν. Clearly, P_ν is a B-submodule of B^m. If M is locally reducible, then each projection P_ν is a direct summand in the socle $S(B^m)$; this means that there exist B-submodules Q_ν of B^m satisfying

$$S(B^m) = P_\nu \oplus Q_\nu, \qquad \text{for all } \nu. \tag{16}$$

LEMMA 3.6. *Given a locally reducible code M, let $\mathbf{g}(D)$ be any sequence in M_ν, with $\mathbf{g}_0 \neq \mathbf{0}$ and $\nu \geqslant 1$. Then there exists a normal sequence $\mathbf{h}(D) \in M_\nu$ such that $\mathbf{h}_0 = \mathbf{g}_0$ holds.*

Proof. We shall successively construct sequences $\mathbf{f}_0(D)$, $\mathbf{f}_1(D)$,..., $\mathbf{f}_{\nu-1}(D)$ in M_ν, the words of $\mathbf{f}_s(D)$ being subject to $\mathbf{f}_{s,0} = \mathbf{g}_0$ and $\mathbf{f}_{s,j} \in Q_{\nu-j}$ for $j = 1, 2, \ldots, s$.

For a given μ, with $1 \leqslant \mu \leqslant \nu$, let $\mathbf{f}_{\mu-1}(D)$ satisfy the above requirements. We first decompose the word $\mathbf{f}_{\mu-1,\mu}$ in agreement with (16); thus we write

$$\mathbf{f}_{\mu-1,\mu} = \mathbf{p}_0 + \mathbf{q}_0, \qquad \text{where} \quad \mathbf{p}_0 \in P_{\nu-\mu}, \quad \mathbf{q}_0 \in Q_{\nu-\mu}.$$

Let $\mathbf{p}(D) = \mathbf{p}_0 + \mathbf{p}_1 D + \cdots + \mathbf{p}_{\nu-\mu-1} D^{\nu-\mu-1}$ be any sequence of $M_{\nu-\mu}$ having initial word $\mathbf{p}_0$ (and appropriate words $\mathbf{p}_1, \ldots, \mathbf{p}_{\nu-\mu-1}$). Define $\mathbf{f}_\mu(D) = \mathbf{f}_{\mu-1}(D) - D^\mu \circ \mathbf{p}(D)$. Clearly, $\mathbf{f}_\mu(D)$ has the required properties.

By this inductive method, taking $\mathbf{f}_0(D) = \mathbf{g}(D)$ to start with, we have constructed a sequence $\mathbf{h}(D) = \mathbf{f}_{\nu-1}(D)$ in M_ν satisfying $\mathbf{h}_0 = \mathbf{g}_0$ and $\mathbf{h}_j \in Q_{\nu-j}$ for each $j \geqslant 1$. It remains to be shown that $\mathbf{h}(D)$ is normal. By (7) and (8) we have

$$a \circ \mathbf{h}(D) = \sum_{i=0}^{\nu-1} (a^{\beta(i)} \mathbf{h}_i) D^i, \tag{17}$$

for all $a \in B$. Given an integer μ $(1 \leqslant \mu \leqslant \nu)$, suppose $a^{\beta(i)}\mathbf{h}_i = \mathbf{0}$ for $i = 0, 1, \ldots, \mu - 1$. Then it follows from (17) that $D^{-\mu} \circ a \circ \mathbf{h}(D)$ belongs to $M_{\nu-\mu}$, so that its initial word $a^{\beta(\mu)}\mathbf{h}_\mu$ belongs to $P_{\nu-\mu}$. Now, by construction, $a^{\beta(\mu)}\mathbf{h}_\mu \in Q_{\nu-\mu}$ holds. So, from $P_s \cap Q_s = (\mathbf{0})$, we deduce $a^{\beta(\mu)}\mathbf{h}_\mu = \mathbf{0}$. Hence it is clear, by induction, that $a\mathbf{h}_0 = \mathbf{0}$ implies $a \circ \mathbf{h}(D) = \mathbf{0}$, which means that $\mathbf{h}(D)$ is normal. ∎

THEOREM 3.7. *Let M be a nonzero semiregular convolutional code which is locally reducible. Then M can be expressed as a direct sum of irreducible $B(D)$-modules each of which is generated by a normal sequence of finite length.*

Proof. As before, we denote by P_ν the projection of M_ν in B^m. From the fact that P_ν is a B-submodule of the socle $S(B^m)$ it follows that $P_{\nu-1}$ is a direct summand in P_ν. Thus, for given $\nu \geqslant 1$, there exist B-modules R_μ satisfying

$$P_\nu = R_1 \oplus R_2 \oplus \cdots \oplus R_\nu ,$$

where some of the R_μ may be zero. Next, let us decompose every $R_\mu \neq (\mathbf{0})$ as a direct sum of irreducible B-modules $R_{\mu,s}$; thus

$$R_\mu = R_{\mu,1} \oplus R_{\mu,2} \oplus \cdots \oplus R_{\mu,t(\mu)} .$$

We now choose an arbitrary nonzero element $\mathbf{g}_{\mu,s}$ in each $R_{\mu,s}$, and, thereafter, any sequence $\mathbf{g}_{\mu,s}(D)$ in M_μ having this $\mathbf{g}_{\mu,s}$ as initial word (of index 0). Then we define the following $B(D)$-module:

$$L_\nu = \sum_{\mu \leqslant \nu} \sum_{s=1}^{t(\mu)} B(D) \circ \mathbf{g}_{\mu,s}(D).$$

Obviously, L_ν is a submodule of $B(D) \circ M_\nu$. Furthermore, it is easy to show, by induction over ν, that M_ν is included in L_ν. Hence L_ν coincides with $B(D) \circ M_\nu$.

On the other hand, applying Lemma 3.6, we know that there exists a normal sequence $\mathbf{h}_{\mu,s}(D)$ in M_μ having $\mathbf{g}_{\mu,s}$ as initial word (for every given s and μ). This yields $\mathbf{h}_{\mu,s}(D) \equiv \mathbf{g}_{\mu,s}(D) \pmod{L_{\mu-1}}$ and, consequently,

$$B(D) \circ M_\nu = L_\nu = \sum_{\mu \leqslant \nu} \sum_{s=1}^{t(\mu)} B(D) \circ \mathbf{h}_{\mu,s}(D). \tag{18}$$

Now our finiteness axiom for convolutional codes means that M equals $B(D) \circ M_\nu$ for a suitable $\nu \geqslant 1$. Hence (18) yields the desired result, by application of Lemmas 3.3 and 3.4. ∎

The normal sequences $\mathbf{h}_{\mu,s}(D)$ constructed as in the proof of Theorem 3.7 will be called *canonical generators* of M. We emphasize their main property. Let $\mathbf{f}(D) \in M_{\nu-1}$ be expressed in the form

$$\mathbf{f}(D) = \sum_{\mu \leqslant \nu} \sum_{s=1}^{t(\mu)} a_{\mu,s}(D) \circ \mathbf{h}_{\mu,s}(D),$$

with $a_{\mu,s}(D) \in B(D)$. Then all terms $a_{\nu,s}(D) \circ \mathbf{h}_{\nu,s}(D)$ must be zero. Using this property we shall now see how canonical generators yield *minimal bases* for convolutional codes (cf. Forney, 1970).

THEOREM 3.8. *Let $G_{\mu,s}(D)$ be an F-basis of the B-module $B \circ \mathbf{h}_{\mu,s}(D)$, where the normal sequences $\mathbf{h}_{\mu,s}(D)$ are canonical generators for a given convolutional code $M = B(D) \circ M_\nu$. Then the collection of $G_{\mu,s}(D)$, with $s \leqslant t(\mu)$ and $\mu \leqslant \nu$, constitutes a minimal basis of M.*

Proof. Consider any elements $a_{\mu,s}(D) = \sum_{i=0}^{\infty} a_{\mu,s,i} D^i$ in $B(D)$ having the property that, for a given μ and s, either $a_{\mu,s}(D) \circ \mathbf{h}_{\mu,s}(D)$ is zero or $a_{\mu,s,i} \circ \mathbf{h}_{\mu,s}(D)$ is nonzero for infinitely many values of i. The first thing we have to show is that the sequence

$$\mathbf{g}(D) = \sum_{\mu,s} a_{\mu,s}(D) \circ \mathbf{h}_{\mu,s}(D)$$

is zero or has no finite length. (This means that the $G_{\mu,s}(D)$ form a "non-catastrophic" basis for M; cf. Massey and Sain, 1968.) Suppose on the contrary that $\mathbf{g}(D)$ is nonzero and has finite length. Let ρ be the largest integer $\leqslant \nu$ such that $a_{\rho,r}(D) \circ \mathbf{h}_{\rho,r}(D)$ is nonzero for some $r \leqslant t(\rho)$. Thus there exists an integer $\lambda \geqslant \rho$ such that $\mathbf{g}(D) \in M_\lambda$ holds, together with $a_{\rho,r,\lambda-\rho+1} \circ \mathbf{h}_{\rho,r}(D) \neq \mathbf{0}$. Define

$$\mathbf{f}(D) = \sum_{\mu,s} \left(\sum_{i>\lambda-\rho} a_{\mu,s,i} D^i \right) \circ \mathbf{h}_{\mu,s}(D).$$

Clearly, $\mathbf{g}(D) - \mathbf{f}(D)$ belongs to M_λ. Hence $\mathbf{f}(D)$ has length $\rho - 1$ (and index $\lambda - \rho + 1$), which implies that it has zero components with respect to the $\mathbf{h}_{\rho,s}(D)$, i.e.,

$$\left(\sum_{i>\lambda-\rho} a_{\rho,s,i} D^i \right) \circ \mathbf{h}_{\rho,s}(D) = \mathbf{0}, \qquad \text{all } s \leqslant t(\rho).$$

So $a_{\rho,s,\lambda-\rho+1} \mathbf{h}_{\rho,s,0} = \mathbf{0}$, whence $a_{\rho,s,\lambda-\rho+1} \circ \mathbf{h}_{\rho,s}(D) = \mathbf{0}$ because $\mathbf{h}_{\rho,s}(D)$ is

normal. This contradiction proves that $\mathbf{g}(D)$ actually has no finite length (unless it is zero).

In order to complete the proof, we have to show that both sums $\sum B\mathbf{h}_{\mu,s,0}$ and $\sum B\mathbf{h}_{\mu,s,\mu-1}$ (taken over s and μ) are direct. The first result holds by construction. We shall now prove the second. Let

$$\sum_{\mu,s} a_{\mu,s}\mathbf{h}_{\mu,s,\mu-1} = \mathbf{0}, \tag{19}$$

for some $a_{\mu,s} \in B$. To these elements $a_{\mu,s}$ we associate the sequence $\mathbf{f}(D)$ in M_ν defined to be

$$\mathbf{f}(D) = \sum_{\mu,s} a_{\mu,s}^{\beta(1-\nu)} \circ (D^{\nu-\mu}\mathbf{h}_{\mu,s}(D)).$$

By (19), the coefficient $\mathbf{f}_{\nu-1}$ is zero, so that $\mathbf{f}(D)$ belongs to $M_{\nu-1}$. Hence $\mathbf{f}(D)$ has zero components with respect to the $\mathbf{h}_{\nu,s}(D)$, i.e.,

$$a_{\nu,s}^{\beta(1-\nu)} \circ \mathbf{h}_{\nu,s}(D) = \mathbf{0}, \qquad \text{all } s \leqslant t(\nu).$$

So $a_{\nu,s}\mathbf{h}_{\nu,s,\nu-1} = \mathbf{0}$, for every s. Iterative use of this argument shows that each term of the sum (19) is zero, which leads to the desired result. ∎

4. Examples of Regular and Semiregular Codes

In this last section, we shall describe a few convolutional codes having the algebraic structure introduced here above. They will be represented by means of appropriate canonical generators $\mathbf{h}(D)$. As usual, the *free distance*, denoted by d_f, will be taken as the measure of the efficiency of the code (cf. Massey, 1968). We recall that d_f is the minimum weight of nonzero sequences in the code. In the examples below, we shall compare d_f to the *Griesmer upper bound* d_G for convolutional codes (cf. Layland and McEliece, 1970).

4.1. *Examples with* $q = 2$, $m = 1$, $n = 9$, $k = 2$ *and* 4

4.1.1. Let G be the noncyclic group of order $r = 9$, whose two generators x and y satisfy $x^3 = y^3 = 1$ and $yx = xy$. In the group algebra B of G over the binary field we define

$$e_1 = (x + x^2)(1 + xy + x^2y^2).$$

It is easily seen that e_1 is an idempotent generator for an irreducible 2-dimensional ideal (= submodule) of B.

Next, we define $\alpha \in \mathrm{Aut}(G)$ by $x^\alpha = x^2$ and $y^\alpha = xy$. Note that α is an involution (i.e., $\alpha^2 = 1$). For $m = 1$ and certain values of ν we shall now explicitly give some normal sequences $\mathbf{h}(D) \in B(D)$, of length ν, whose initial word is $\mathbf{h}_0 = e_1$. According to Theorem 3.2, we only have to specify the endomorphisms A_i, which here simply are scalars in the algebra B. In the examples below, A_i is of the form $x^{s(i)}$, for some $s(i) \in \{0, 1, 2, \infty\}$, where x^∞ stands for 0. Thus we write

$$\mathbf{h}(D) = \sum_{i=0}^{\nu-1} (e_1 x^{s(i)})^{\alpha^i} D^i, \qquad \text{with } s(0) = 0, \quad s(\nu - 1) \neq \infty.$$

By Lemma 3.3, the normal sequence $\mathbf{h}(D)$ generates a binary (9,2) convolutional code $M = B(D) \circ \mathbf{h}(D)$ which is an irreducible left ideal (= submodule) of the algebra $B(D)$. Since G is Abelian and α is an involution, M is of the *alternating type*, which makes the computation of the free distance rather easy (cf. Piret, 1975). In Table I we give, for $\nu = 4, 5, \ldots, 9$, a sequence $\mathbf{h}(D)$ which is a canonical generator for a code M achieving or nearly achieving the Griesmer bound. It is interesting to observe that, in the case $\nu = 8$, no optimal code can be obtained without taking some $s(i) = \infty$.

TABLE I

Some Binary (9, 2) Regular Convolutional Codes

ν	$(s(i); 0 \leqslant i \leqslant \nu - 1)$	d_f	d_G
4	(0, 0, 0, 1)	24	24
5	(0, 0, 0, 0, 1)	28	28
6	(0, 0, 0, 0, 1, 2)	32	32
7	(0, 0, 0, 1, 2, 1, 1)	36	38
8	(0, 0, ∞, 0, 0, 1, 2, 1)	42	42
9	(0, 0, ∞, 1, 1, 2, 1, 0, 0)	46	48

4.1.2. In the same group algebra B, consider the idempotent

$$e_2 = (x + x^2)(1 + y + y^2).$$

It is easily seen that Be_2 is an irreducible 2-dimensional ideal of B having only 0 in common with Be_1.

Here we choose the automorphism α of G given by $x^\alpha = y^2$ and $y^\alpha = x$.

From e_1 and e_2 we construct normal sequences $\mathbf{h}_1(D)$ and $\mathbf{h}_2(D)$ in $B(D)$, having length $\nu = 4$, as follows:

$$\mathbf{h}_1(D) = e_1 + e_1{}^{\alpha}D + e_1^{\alpha^2}D^2 + (e_1x)^{\alpha^3}D^3,$$

$$\mathbf{h}_2(D) = e_2 + e_2{}^{\alpha}D + (e_2x^2)^{\alpha^3}D^3.$$

By Lemmas 3.3 and 3.4, the sum $M = B(D) \circ \mathbf{h}_1(D) + B(D) \circ \mathbf{h}_2(D)$ is a direct sum of irreducible left ideals of $B(D)$. Thus M is a binary (9,4) convolutional code. In fact, $\mathbf{h}_1(D)$ and $\mathbf{h}_2(D)$ are canonical generators for M. Moreover, it can be verified that M has free distance $d_f = 16$ and is optimal in the class of regular codes of type $(G, \alpha, 1)$ having dimension $k = 4$ and generators of length $\nu = 4$. For these parameters, the Griesmer bound is $d_G = 18$.

4.2. *Examples with Nonabelian Groups, and with $m > 1$*

4.2.1. Let G be the noncyclic group of order $r = 6$, whose two generators x and y satisfy $x^2 = y^3 = 1$ and $yx = xy^2$. It is well known that $\mathrm{Aut}(G)$ is isomorphic to G itself; thus, for given α in G, the mapping $z \mapsto z^{\alpha} = \alpha^{-1}z\alpha$ defines a typical automorphism of G. By Theorem 2.3, for any group algebra $B = FG$, the F-algebra $(B(D), +, o)$ only depends, up to isomorphism, on the conjugacy class to which α belongs. So there are essentially three choices for α, namely $\alpha = 1$, $\alpha = x$, and $\alpha = y$.

We now choose $F = GF(2)$. Note that B is not semisimple. We shall make use of the element $e \in B$ given by

$$e = 1 + xy + xy^2 + y^2.$$

It is quite easy to check that e is idempotent and generates a 2-dimensional irreducible left ideal of B. To each of the three inequivalent $\alpha \in \mathrm{Aut}(G)$ let us associate a normal sequence $\mathbf{h}(D)$ of length $\nu = 3$ in $B(D)$, written in the form (14), as follows:

$$\mathbf{h}(D) = e + e^{\alpha}D + (ey)^{\alpha^2}D^2,$$

$$\mathbf{h}(D) = e + (ey^2)^{\alpha}D + (ey)^{\alpha^2}D^2,$$

$$\mathbf{h}(D) = e + (ey^2)^{\alpha}D + e^{\alpha^2}D^2,$$

for $\alpha = 1$, x and y, respectively. In each case, $\mathbf{h}(D)$ is a canonical generator for an irreducible regular (6,2) code having optimal free distance $d_f = d_G = 12$. To show connection with the standard description of convolutional

codes, we give a generator matrix for the third case (when the successive columns correspond to the elements 1, y, y^2, x, xy and xy^2 of G), namely

$$\begin{bmatrix} 1+D^2 & D & 1+D+D^2 & D+D^2 & 1 & 1+D+D^2 \\ 1+D+D^2 & 1+D^2 & D & 1 & 1+D+D^2 & D+D^2 \end{bmatrix}.$$

4.2.2. For the same group G of order 6 but now with $F = GF(5)$, the group algebra B is semisimple. In this B let us choose the idempotent

$$e = 2 + 3x + 2xy + 3y^2.$$

It generates a 2-dimensional irreducible left ideal of B. Here we define $\alpha \in \mathrm{Aut}(G)$ by $z^\alpha = y^{-1}zy$. Then the normal sequence

$$\mathbf{h}(D) = e + (e(2 + y^2))^\alpha D,$$

of length $\nu = 2$, is a canonical generator for an irreducible regular (6,2) convolutional code over F. Its free distance is $d_f = 10$ and so achieves the Griesmer bound.

4.2.3. In our last example we take $G \cong \mathbb{Z}_5$, $\alpha = 1$, $m = 3$, and $F = GF(2)$. In the group algebra $B = FG$, let us define

$$e = x + x^2 + x^3 + x^4, \qquad \text{and} \qquad a = 1 + x,$$

where x is a generator of G. Clearly, the triple $\mathbf{h} = (e, ea, ea^2)$ generates a 4-dimensional irreducible submodule of B^3. Then we construct a normal sequence $\mathbf{h}(D)$ of length $\nu = 3$ in $B^3(D)$, having $\mathbf{h}$ as initial word, namely

$$\mathbf{h}(D) = (e, ea, ea^2) + (e, ea^2, ea)\, D + (ea^4, ea^5, ea^9)\, D^2.$$

It turns out that $\mathbf{h}(D)$ is a canonical generator for an irreducible semiregular (15,4) convolutional code $M = B(D) \circ \mathbf{h}(D)$ having free distance $d_f = 24$. This code M is optimal (for the parameters $q = 2$, $n = 15$, $k = 4$, $\nu = 3$), because $d_f = d_G$ holds.

Acknowledgment

The authors are indebted to the reviewer for useful remarks concerning the organization of the present paper.

Received: March 14, 1975; revised: April 15, 1976

REFERENCES

CHEN, C. L., PETERSON, W. W., AND WELDON, E. J. (1969), Some results on quasicyclic codes, *Inform. Contr.* **15**, 407–423.

CURTIS, C. W., AND REINER, I. (1962), "Representation Theory of Finite Groups and Associative Algebras," Wiley, New York.

FORNEY, G. D. (1970), Convolutional codes I: Algebraic structure, *IEEE Trans. Information Theory* **IT–16**, 720–738.

LAYLAND, J., AND MCELIECE, R. J. (1970), An upper bound on the free distance of a tree code, *in* "Jet Propulsion Laboratory Space Program Summary 37–62," Vol. 3, pp. 63–64.

MACWILLIAMS, F. J. (1967), Codes and ideals in group algebras, *in* "Combinatorial Mathematics and Its Applications" (R. C. Bose and T. A. Dowling Eds.), pp. 317–328. The Univ. North Carolina Press, Chapel Hill.

MACWILLIAMS, F. J. (1970), Binary codes which are ideals in the group algebra of an abelian group, *Bell Syst. Tech. J.* **49**, 987–1011.

MASSEY, J. L. (1968), Some algebraic and distance properties of convolutional codes, *in* "Proceedings of the Symposium on Error Correcting Codes," Univ of Wisconsin, Madison.

MASSEY, J. L., AND SAIN, M. K. (1968), Inverses of linear sequential circuits, *IEEE Trans. Computers* **C–17**, 330–337.

PIRET, P. (1975), On a class of alternating cyclic convolutional codes, *IEEE Trans. Information Theory* **IT–21**, 64–69.

PIRET, P. (1976), Structure and constructions of cyclic convolutional codes, *IEEE Trans. Information Theory* **IT–22**, 147–155.

WIELANDT, H. (1964), "Finite Permutation Groups," Academic Press, New York.